Hardening Windows Server 2025 : guide CIS Benchmark complet

> Guide complet de durcissement Windows Server 2025 : CIS Benchmark Level 1/2, Secured-Core, GPO, audit events, PowerShell et checklist 40 points.

Windows Server 2025 introduit des capacités de sécurité natives significativement améliorées par rapport à ses prédécesseurs : Secured-Core Server, Credential Guard activé par défaut, SMB over QUIC, et une intégration renforcée avec les fonctionnalités de sécurité du firmware UEFI. Pour autant, une installation fraîche de Windows Server 2025 avec les paramètres par défaut est loin d'être sécurisée au niveau requis pour les environnements de production exposés. Le CIS (Center for Internet Security) a publié son Benchmark pour Windows Server 2025, définissant plus de 350 contrôles répartis en deux niveaux (L1 et L2). Ce guide technique couvre l'intégralité du processus de durcissement : des nouveautés sécurité natives à la configuration des stratégies d'audit, en passant par la désactivation des services dangereux, les GPO recommandées, le chiffrement et la gestion des correctifs. Chaque section inclut des commandes PowerShell vérifiées pour automatiser ou valider les contrôles. Une checklist en 40 points synthétise les actions prioritaires. Ce guide s'adresse aux administrateurs système, ingénieurs sécurité et équipes SOC qui déploient ou sécurisent des serveurs Windows Server 2025 en environnement Active Directory ou en workgroup isolé.

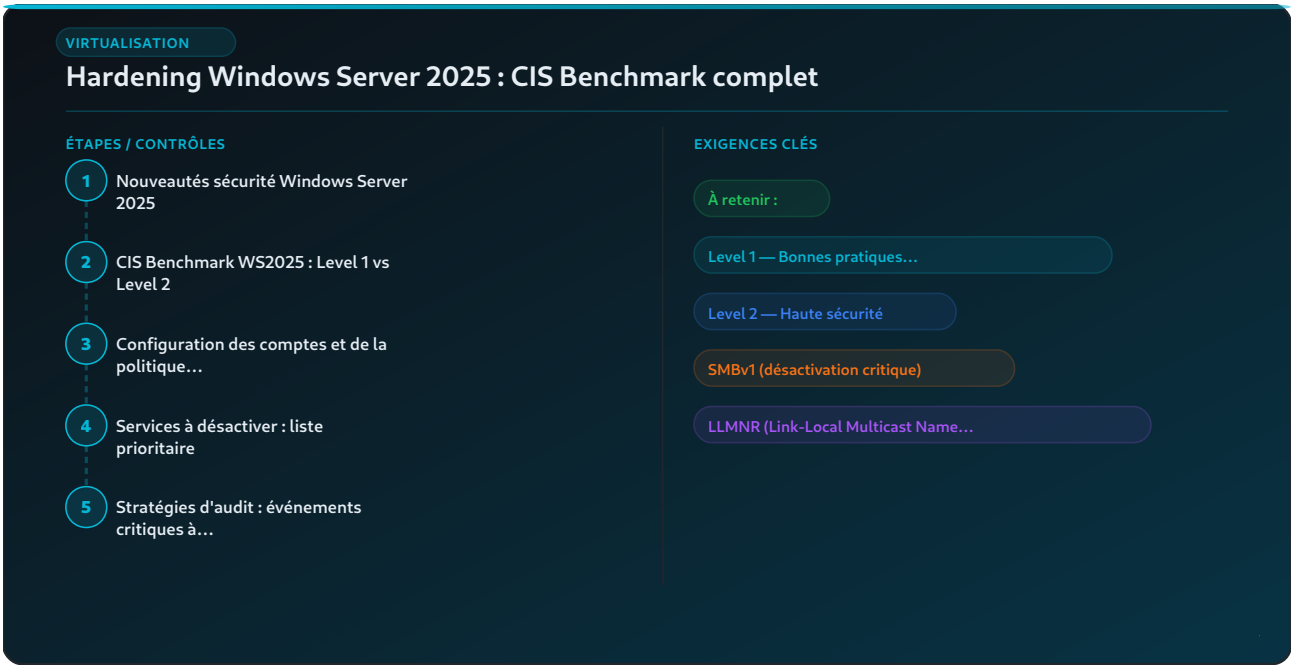
À RETENIR

À retenir :

Windows Server 2025 active Credential Guard et le Secure Boot par défaut sur le matériel compatible, mais de nombreux paramètres dangereux (LLMNR, NetBIOS, SMBv1) restent actifs par défaut.

Le CIS Benchmark Level 1 est applicable dans tous les environnements ; Level 2 ajoute des contrôles plus restrictifs adaptés aux serveurs à haute valeur ou exposés.

> La désactivation de SMBv1, LLMNR, NetBIOS over TCP/IP et Print Spooler (hors serveurs d'impression) est le premier niveau de durcissement à appliquer avant toute mise en production.
>
> L'audit des événements 4624/4625/4648/4768/4771/4776 est fondamental pour la détection des attaques Pass-the-Hash, Kerberoasting et AS-REP Roasting par votre SIEM/SOC.



Nouveautés sécurité Windows Server 2025

Secured-Core Server

Secured-Core Server est une certification matérielle et logicielle introduite avec Windows Server 2019 et renforcée dans la version 2025. Elle garantit que le serveur utilise les fonctionnalités UEFI Secure Boot, TPM 2.0, HVCI (Hypervisor-Protected Code Integrity) et le mode de protection du firmware DRTM (Dynamic Root of Trust for Measurement). Sur un matériel certifié Secured-Core Server 2025 (Dell PowerEdge, HPE ProLiant Gen11, Lenovo ThinkSystem), ces protections sont activées par défaut et ne peuvent pas être désactivées depuis

l'OS. Cette architecture protège contre les rootkits firmware et les attaques persistantes au niveau du bootloader.

Credential Guard natif et VBS

Windows Server 2025 active automatiquement Credential Guard sur les systèmes compatibles VBS (Virtualization-Based Security). Credential Guard isole les secrets NTLM et Kerberos dans un environnement VSM (Virtual Secure Mode) protégé par l'hyperviseur, les rendant inaccessibles même depuis le contexte SYSTEM. Cette protection rend les attaques Pass-the-Hash et Pass-the-Ticket significativement plus difficiles. La vérification de l'activation se fait via `msinfo32.exe` (section "Virtualization-based security") ou PowerShell.

```
 # Vérifier l'état de Credential Guard et VBS
Get-ComputerInfo | Select-Object -Property DeviceGuardSmartStatus, DeviceGuardRequiredSecurityPro
```

SMB over QUIC

Windows Server 2025 supporte SMB over QUIC, permettant le partage de fichiers SMB via le protocole QUIC (UDP 443) sans VPN. Ce protocole offre un chiffrement TLS 1.3 natif, une résistance aux interruptions réseau et l'élimination du port SMB traditionnel (TCP 445) pour les accès distants. SMB over QUIC nécessite une PKI interne pour la distribution des certificats serveur. Il est recommandé de l'activer pour les accès distants des travailleurs mobiles tout en continuant à restreindre TCP 445 aux flux internes uniquement.

CIS Benchmark WS2025 : Level 1 vs Level 2

Le CIS Benchmark Windows Server 2025 définit deux profils de configuration :

⚡ **Retour terrain**

Dans les projets de virtualisation, la sécurisation de l'hyperviseur lui-même est souvent négligée au profit de la sécurisation des VMs. Sur le dernier audit d'infrastructure que j'ai réalisé, l'interface de gestion Proxmox était accessible depuis le VLAN utilisateurs sans restriction, avec un compte admin utilisant le mot de passe par défaut. Une VM compromise aurait pu compromettre l'ensemble du cluster. La surface d'attaque de l'hyperviseur doit être traitée avec le même niveau d'exigence que les systèmes les plus critiques.

Level 1 — Bonnes pratiques fondamentales : Ensemble de configurations recommandées pour tous les environnements Windows Server 2025. Ces contrôles offrent un rapport sécurité/impact opérationnel favorable et ne devraient pas perturber les fonctionnalités essentielles d'un serveur correctement configuré. Le Level 1 est l'objectif minimum pour tout serveur en production.

Level 2 — Haute sécurité : Contrôles additionnels pour les environnements nécessitant une posture de sécurité renforcée (serveurs DMZ, serveurs exposés à Internet, serveurs contenant des données très sensibles). Ces contrôles peuvent restreindre certaines fonctionnalités et nécessitent un test approfondi avant déploiement en production. Exemples : désactivation complète de RDP sur certains profils, restrictions PowerShell renforcées, audit de succès ET d'échec sur toutes les catégories.

Le choix du niveau dépend du rôle du serveur, de son exposition réseau et des exigences de conformité (ISO 27001, NIS2, PCI-DSS). Pour un contrôleur de domaine ou un serveur de fichiers sensible, le Level 2 est recommandé. Pour un serveur applicatif interne standard, le Level 1 est suffisant.

Configuration des comptes et de la politique de mots de passe

Renommer et désactiver les comptes par défaut

Le compte Administrateur intégré et le compte Invité sont des cibles prioritaires pour les attaquants. Le CIS Benchmark recommande de renommer le compte Administrateur avec un nom non évident, de désactiver le compte Invité (déjà désactivé par défaut mais à vérifier), et de créer des comptes nommés spécifiques à chaque administrateur pour garantir l'imputabilité des actions dans les logs.

```
 # Renommer le compte Administrateur intégré
Rename-LocalUser -Name "Administrator" -NewName "svc-admin-srv01"
# Vérifier le statut du compte Invité
Get-LocalUser -Name "Guest" | Select-Object Name, Enabled, Description
# Désactiver si activé
Disable-LocalUser -Name "Guest"
```

Politique de mots de passe (GPO)

Dans un environnement Active Directory, la politique de mot de passe s'applique via GPO ou via les Fine-Grained Password Policies (PSO) pour des groupes spécifiques. Le CIS Benchmark Level 1 pour WS2025 recommande : longueur minimale 14 caractères, historique 24 mots de passe, âge maximum 60 jours, complexité activée. Pour les comptes de service, utiliser des GMSA (Group Managed Service Accounts) avec rotation automatique des mots de passe plutôt que des comptes standards.

```
 # Configurer la politique de mots de passe locale (hors AD)
secedit /export /cfg C:\secpol.cfg
# Modifier les valeurs dans le fichier puis réimporter :
# MinimumPasswordLength = 14
# PasswordHistorySize = 24
# MaximumPasswordAge = 60
# PasswordComplexity = 1
secedit /configure /db secedit.sdb /cfg C:\secpol.cfg /areas SECURITYPOLICY
```

Politique de verrouillage de compte

Le CIS recommande : seuil de verrouillage à 5 tentatives, durée de verrouillage de 15 minutes minimum, réinitialisation du compteur après 15 minutes. Ces paramètres protègent contre les attaques par force brute sur les protocoles NTLM et les interfaces web d'authentification.

Services à désactiver : liste prioritaire

Windows Server 2025 inclut de nombreux services activés par défaut qui augmentent la surface d'attaque sans apporter de valeur dans la plupart des configurations. Voici les services à désactiver en priorité :

SMBv1 (désactivation critique) : SMBv1 est le protocole exploité par EternalBlue (WannaCry, NotPetya). Il est désactivé par défaut dans WS2025 mais peut être réactivé par erreur. À vérifier systématiquement.

```
 # Vérifier et désactiver SMBv1
Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
# Désinstaller le composant Windows Features
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart
```

LLMNR (Link-Local Multicast Name Resolution) : LLMNR répond aux requêtes de résolution de noms locaux via multicast. C'est le protocole exploité par Responder pour capturer des hashes NTLM via des poisoning attacks. À désactiver via GPO : Computer Configuration > Administrative Templates > Network > DNS Client > Turn off multicast name resolution = Enabled.

NetBIOS over TCP/IP : NetBIOS est un protocole hérité exploitable pour la capture de credentials NTLM. À désactiver sur toutes les interfaces réseau via les propriétés avancées TCP/IP, ou via DHCP option 001 = 0x2.

Print Spooler (hors serveurs d'impression dédiés) : La vulnérabilité PrintNightmare (CVE-2021-34527) et ses variantes ont démontré la dangerosité du service Print Spooler sur les

contrôleurs de domaine et serveurs critiques. Désactiver sur tous les serveurs sauf les serveurs d'impression dédiés.

```
 # Désactiver le Print Spooler
Stop-Service -Name Spooler -Force
Set-Service -Name Spooler -StartupType Disabled

# Désactiver LLMNR via Registry (si GPO non disponible)
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" -Name "EnableMult

# Désactiver NetBIOS sur toutes les interfaces via WMI
$adapters = Get-WmiObject Win32_NetworkAdapterConfiguration | Where-Object {$_.IPEnabled}
$adapters | ForEach-Object { $_.SetTcpipNetbios(2) }
```

Autres services à évaluer : Remote Registry (désactiver si non utilisé pour la gestion à distance), Telnet Client (désinstaller), TFTP Client (désinstaller), Simple Network Management Protocol (SNMP, désactiver si non utilisé ou configurer avec SNMPv3).

Stratégies d'audit : événements critiques à surveiller

Un système Windows Server 2025 correctement audité génère les logs nécessaires pour détecter les attaques Active Directory, les mouvements latéraux et les escalades de privilèges. Le CIS Benchmark définit précisément les catégories d'audit à activer.

Catégories d'audit recommandées

```
 # Configurer l'audit via auditpol (à exécuter sur chaque serveur ou via GPO)
# Connexions de compte
auditpol /set /subcategory:"Credential Validation" /success:enable /failure:enable
auditpol /set /subcategory:"Kerberos Authentication Service" /success:enable /failure:enable
auditpol /set /subcategory:"Kerberos Service Ticket Operations" /success:enable /failure:enable
# Gestion de compte
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Security Group Management" /success:enable /failure:enable
# Connexion/déconnexion
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Logoff" /success:enable /failure:enable
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
# Accès aux objets
auditpol /set /subcategory:"File System" /failure:enable
# Utilisation des privilèges
auditpol /set /subcategory:"Sensitive Privilege Use" /success:enable /failure:enable
# Changements de politique
auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable
```

Événements Windows critiques pour le SOC

Les identifiants d'événements suivants sont essentiels pour votre SIEM :

4624 : Connexion réussie — surveiller les types 3 (réseau), 10 (accès distant interactif) depuis des IP inconnues

4625 : Échec de connexion — détecter les brute force (nombreux 4625 suivis d'un 4624)

4648 : Connexion avec credentials explicites (runas, Pass-the-Hash)

4768 : Demande de TGT Kerberos — surveiller les demandes depuis des IP non-membres du domaine

4771 : Pré-authentification Kerberos échouée — signal AS-REP Roasting

4776 : Validation de credentials NTLM — surveiller les authentifications NTLM sur les DC (devrait être rare en environnement moderne)

4720/4732/4756 : Création de compte, ajout à groupe Security/Universal — escalade de privilèges

GPO recommandées : LSASS, Credential Guard, Device Guard

Protection LSASS contre le dumping de mémoire

LSASS (Local Security Authority Subsystem Service) stocke les credentials en mémoire et est la cible principale des outils de dumping (Mimikatz, ProcDump). Windows Server 2025 offre plusieurs couches de protection :

```
 # Activer la protection LSASS (PPL - Protected Process Light)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RunAsPPL" -Value 1 -Ty
# Activer LSASS Audit Mode (pour détecter les tentatives d'accès)
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution O
# Via GPO : Computer Configuration > Windows Settings > Security Settings > Local Policies > Secu
# "LSASS.exe: Protected Process" = Enabled with UEFI Lock
```

Windows Defender Credential Guard

Sur les systèmes non-Secured-Core où Credential Guard n'est pas activé par défaut, activez-le via GPO : Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security = Enabled, avec "Credential Guard Configuration" = Enabled with UEFI lock.

Windows Defender Application Control (WDAC / Device Guard)

WDAC remplace AppLocker et permet de définir des politiques contrôlant quel code peut s'exécuter sur le serveur. Une politique WDAC en mode "Allow Microsoft" bloque tous les binaires non signés par Microsoft, réduisant drastiquement la surface d'exécution de malwares. Sur les serveurs à haute valeur (DC, PKI, serveurs de fichiers critiques), WDAC est fortement recommandé.

Pare-feu Windows Defender : configuration minimale

Le pare-feu Windows Defender doit être activé sur les trois profils (Domain, Private, Public) avec une politique par défaut de blocage des connexions entrantes. Sur les serveurs, seuls les ports nécessaires au rôle du serveur doivent être ouverts en entrée.

```
 # S'assurer que le pare-feu est actif sur tous les profils
Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled True
# Vérifier la politique par défaut (doit être Block pour Inbound)
Get-NetFirewallProfile | Select-Object Name, DefaultInboundAction, DefaultOutboundAction
# Exemple : autoriser RDP uniquement depuis le réseau de gestion
New-NetFirewallRule -DisplayName "RDP-ManagementNetwork" -Direction Inbound `
  -Protocol TCP -LocalPort 3389 -RemoteAddress "10.0.100.0/24" -Action Allow
# Bloquer RDP depuis toutes les autres sources
New-NetFirewallRule -DisplayName "RDP-Block-All" -Direction Inbound `
  -Protocol TCP -LocalPort 3389 -Action Block
```

Chiffrement : BitLocker, SMB et TLS 1.3

BitLocker avec TPM 2.0

BitLocker protège les données au repos contre les accès physiques non autorisés. Sur Windows Server 2025, BitLocker est disponible sur toutes les éditions et supporte TPM 2.0 pour une protection sans PIN (adaptée aux serveurs headless). La configuration recommandée utilise XTS-AES 256 bits. Les clés de récupération doivent être stockées dans Active Directory ou Azure AD (pour les environnements hybrides).

```
 # Activer BitLocker sur le volume système avec TPM
Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -TpmProtector
# Sauvegarder la clé de récupération en AD
Backup-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId (Get-BitLockerVolume -MountPoint "C
```

Restriction TLS : désactiver les versions obsolètes

Windows Server 2025 supporte TLS 1.3 nativement. Les versions TLS 1.0 et 1.1 doivent être désactivées. La configuration se fait via le registre ou via les paramètres Schannel.

```
 # Désactiver TLS 1.0 et 1.1 (serveur et client)
$protocols = @("TLS 1.0", "TLS 1.1")
foreach ($proto in $protocols) {
    $path = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\$proto"
    New-Item -Path "$path\Server" -Force | Out-Null
    Set-ItemProperty -Path "$path\Server" -Name "Enabled" -Value 0 -Type DWord
    Set-ItemProperty -Path "$path\Server" -Name "DisabledByDefault" -Value 1 -Type DWord
    New-Item -Path "$path\Client" -Force | Out-Null
    Set-ItemProperty -Path "$path\Client" -Name "Enabled" -Value 0 -Type DWord
    Set-ItemProperty -Path "$path\Client" -Name "DisabledByDefault" -Value 1 -Type DWord
}
```

Gestion des correctifs : WSUS vs Windows Update for Business

La gestion des correctifs sur Windows Server 2025 repose sur deux approches selon la taille de l'organisation. WSUS (Windows Server Update Services) offre un contrôle granulaire des mises à jour avec approbation manuelle, adapté aux grandes organisations avec des processus de qualification formels. Windows Update for Business (WUfB) s'appuie sur les GPO pour différer les mises à jour de 0 à 35 jours, adapté aux environnements plus agiles.

Les délais recommandés par le CIS : pour les mises à jour critiques et de sécurité, déploiement en production dans les 30 jours suivant la publication. Pour les serveurs exposés à Internet ou contenant des données critiques, viser 7 à 14 jours pour les correctifs critiques. Les mises à jour qualité mensuelles ("Patch Tuesday") doivent être testées en environnement de pré-production avant déploiement en production.

Durcissement IIS si présent

Sur les serveurs Windows Server 2025 hébergeant IIS, des mesures de durcissement spécifiques s'appliquent. Désactivez les méthodes HTTP non nécessaires (WebDAV si non utilisé, TRACE, OPTIONS). Configurez les headers de sécurité : X-Content-Type-Options: nosniff, X-Frame-Options: SAMEORIGIN, Strict-Transport-Security avec une durée d'au moins 1 an, Content-Security-Policy adapté à l'application. Supprimez les informations de version dans les headers Server et X-Powered-By.

```
 # Supprimer le header "Server" révélant la version IIS
Import-Module WebAdministration
Set-WebConfigurationProperty -PSPath "IIS:" -Filter "system.webServer/security/requestFiltering"
# Ajouter les headers de sécurité
Add-WebConfigurationProperty -PSPath "IIS:" -Filter "system.webServer/httpProtocol/customHeaders"
Add-WebConfigurationProperty -PSPath "IIS:" -Filter "system.webServer/httpProtocol/customHeaders"
```

Pour les aspects Active Directory, notre guide sur le durcissement AD FS et les recommandations Microsoft pour Active Directory sont des lectures complémentaires essentielles. Les Authentication Policy Silos permettent de restreindre l'utilisation des comptes privilégiés. Notre article sur Credential Guard dans Windows Server 2025 approfondit ce mécanisme de protection des credentials.

Les références officielles incluent le CIS Benchmark Windows Server sur cisecurity.org et la documentation Microsoft sur le Secured-Core Server.

Checklist de durcissement Windows Server 2025 — 40 points

Comptes et authentification (8 points) :

Renommer le compte Administrateur intégré

Désactiver le compte Invité

Longueur minimale mots de passe : 14 caractères

Historique mots de passe : 24

Seuil de verrouillage : 5 tentatives

MFA activé pour tous les comptes administrateurs

Comptes de service : utiliser GMSA

Désactiver les comptes inactifs depuis plus de 30 jours

Services (7 points) :

SMBv1 désactivé et désinstallé

LLMNR désactivé via GPO

NetBIOS over TCP/IP désactivé

Print Spooler désactivé (hors serveurs impression)

Remote Registry désactivé si non nécessaire

Telnet/TFTP désinstallés

SNMP : version 3 uniquement ou désactivé

Audit et journalisation (6 points) :

Audit des connexions réussies et échouées activé

Audit de la validation des credentials Kerberos/NTLM

Audit de la gestion des comptes et groupes

Audit des changements de politique de sécurité

Taille des journaux : Security 1 Go minimum, Application 512 Mo

Centralisation des logs vers SIEM configurée

Protection des credentials (5 points) :

Credential Guard activé

LSASS RunAsPPL activé

WDigest désactivé (pas de stockage des mots de passe en clair)

Restricted Admin Mode pour RDP activé

Comptes Admin locaux différents sur chaque serveur (LAPS)

Réseau et pare-feu (6 points) :

Pare-feu Windows activé sur les 3 profils

Politique par défaut : bloquer les connexions entrantes

RDP restreint aux réseaux de gestion uniquement

SMB TCP 445 restreint aux flux autorisés

TLS 1.0/1.1 désactivés

Suites cryptographiques faibles désactivées (RC4, DES, 3DES)

Chiffrement et mises à jour (4 points) :

BitLocker activé sur tous les volumes

Clés de récupération BitLocker stockées en AD

Politique de mise à jour : correctifs critiques sous 30 jours

Windows Defender Antivirus activé et à jour

Sécurité applicative (4 points) :

WDAC configuré (Application Control)

PowerShell : mode Constrained Language activé sur les serveurs non-admin

Script Block Logging activé pour PowerShell

IIS durci si présent (headers sécurité, versions masquées)

FAQ — Questions fréquentes sur le hardening Windows Server 2025

Le CIS Benchmark Level 2 peut-il casser des applications existantes ?

Oui, le Level 2 peut provoquer des dysfonctionnements sur certaines applications legacy. Les contrôles Level 2 les plus susceptibles de causer des incompatibilités incluent : la restriction des algorithmes cryptographiques (certaines applications anciennes nécessitent encore RC4 ou des versions TLS obsolètes), les politiques de restriction d'applications WDAC (les applications non-signées ou signées avec des certificats non reconnus seront bloquées), et les paramètres de durée

de session Kerberos renforcés. Il est impératif de tester le Level 2 en environnement de développement/staging avec toutes les applications métier avant tout déploiement en production. Une approche progressive (déployer Level 1 d'abord, puis activer les contrôles Level 2 un par un) est recommandée.

Comment auditer rapidement la conformité CIS d'un parc de serveurs existant ?

Plusieurs outils permettent d'évaluer automatiquement la conformité CIS. CIS-CAT Pro (outil officiel CIS, payant) génère un rapport détaillé score par score. Microsoft Security Compliance Toolkit inclut des scripts PowerShell et des templates GPO alignés sur les recommandations Microsoft. Pour une approche open source, l'outil Lynis (sur Windows via WSL) ou les scripts de vérification disponibles sur GitHub (CIS-Hardened-Windows) permettent une évaluation rapide. En environnement Microsoft Defender for Endpoint, la fonctionnalité "Configuration Score" dans le portail Microsoft 365 Security fournit une évaluation continue de la posture de sécurité des endpoints.

Comment gérer les mots de passe des comptes Administrateur locaux sur des centaines de serveurs ?

Microsoft LAPS (Local Administrator Password Solution), désormais intégré nativement à Windows Server 2025 et Windows 11 sous le nom "Windows LAPS", est la réponse officielle à ce problème. Windows LAPS génère automatiquement un mot de passe aléatoire unique pour le compte Administrateur local de chaque machine et le stocke dans Active Directory (attribut ms-LAPS-Password) ou Azure AD. Le mot de passe est automatiquement renouvelé selon une période configurable. Les administrateurs autorisés peuvent récupérer le mot de passe via ADUC, PowerShell (Get-LapsADPassword) ou le portail Intune. Cette solution élimine le risque de réutilisation de mot de passe Administrateur local entre machines (lateral movement via Pass-the-Hash sur les comptes locaux).

Sources et références

[ANSSI — Recommandations de sécurité relatives aux hyperviseurs]

[NIST SP 800-125 — Guide to Security for Full Virtualization]

